

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-005777

(43)Date of publication of application : 12.01.2001

(51)Int.Cl.

G06F 15/00  
G06F 13/00  
H04L 9/32

(21)Application number : 11-177619

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 24.06.1999

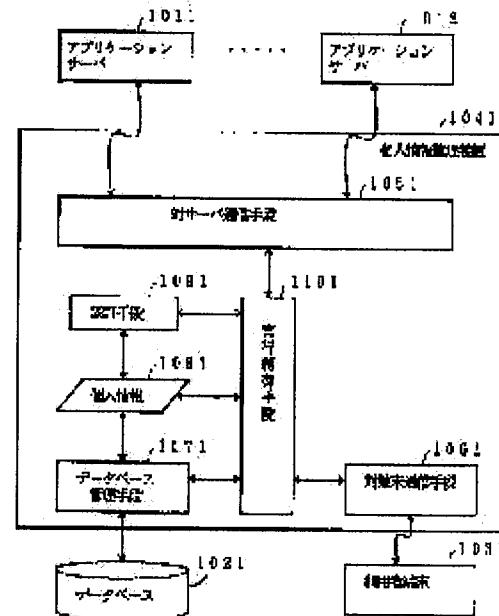
(72)Inventor : SATO KATSUFUMI

## (54) PERSONAL INFORMATION MANAGEMENT DEVICE

(57)Abstract:

**PROBLEM TO BE SOLVED:** To lighten the operation burden on a user who use plural application services by adding authentication information on the basis of personal information obtained by the authentication of the user to transmit data to an application server.

**SOLUTION:** A terminal communication means 1061 monitors the reception of a connection request from a user terminal 1031 and obtains personal information 1081 of a user from a database 1021 by using a database managing means 1071 when receiving a connection request, and an authenticating means 1091 performs authentication. When the authentication is successful, a child process for the user is actuated and the personal information 1081 is passed to the child process. The child process starts processing to monitor data reception by the terminal communication means 1061 and a server communication means 1051. When data are received, its transmission destination is confirmed and transmits data to application servers 1011 to 1012 are given authentication information and sent from the server communication means 1051.



(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-5777

(P2001-5777A)

(43)公開日 平成13年1月12日 (2001.1.12)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テ-マコード <sup>*</sup> (参考)
G 06 F 15/00	3 1 0	G 06 F 15/00	3 1 0 A 5 B 0 8 5
13/00	3 5 4	13/00	3 5 4 Z 5 B 0 8 9
H 04 L 9/32		H 04 L 9/00	6 7 5 A 5 J 1 0 4

審査請求 未請求 請求項の数8 O L (全26頁)

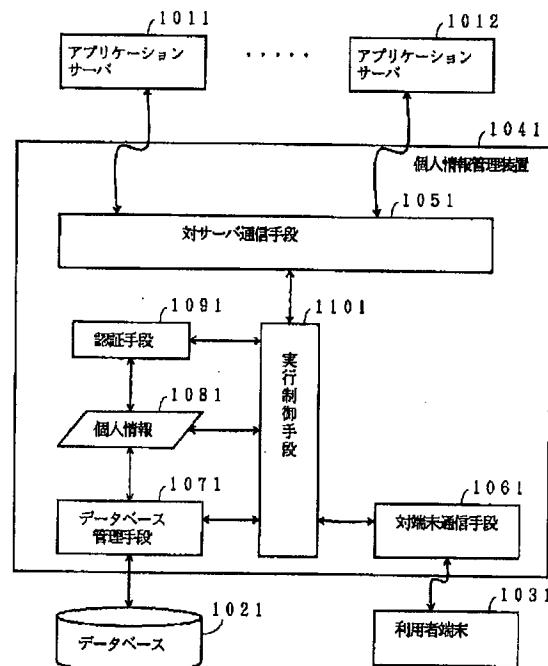
(21)出願番号	特願平11-177619	(71)出願人	000005821 松下電器産業株式会社 大阪府門真市大字門真1006番地
(22)出願日	平成11年6月24日 (1999.6.24)	(72)発明者	佐藤 克文 宮城県仙台市泉区明通二丁目5番地 株式会社松下通信仙台研究所内
特許法第30条第1項適用申請有り 1999年1月21日 社団法人情報処理学会発行の「情報処理学会研究報告 V o L. 99 No. 4」に発表			(74)代理人
			100079544 弁理士 斎藤 繁 Fターム(参考) 5B085 AC03 AE23 BG07 5B089 GA11 GB03 JA11 JB22 KA01 KB13 KC44 KC58 5J104 AA07 KA01 KA04 MA02 NA38 PA07

(54)【発明の名称】 個人情報管理装置

(57)【要約】

【課題】複数のアプリケーションサーバに対し使用する個人情報を一元的に管理してアプリケーションサービス要求毎の操作負担を軽減する個人情報管理装置を提供すること。

【解決手段】ネットワークを介し、特定の利用者を対象にアプリケーションサービスを提供するアプリケーションサーバ1011、1012と、利用者情報を出力しアプリケーションサーバ情報を入力する利用者端末1031とが接続されたコンピュータシステムにおいて、アプリケーションサーバとの通信を行う対サーバ通信手段1051と、利用者端末との通信を行う対端末通信手段1061と、利用者の個人情報を格納するデータベース1021と、データベースに対し個人情報の変更、入出力等を操作するデータベース管理手段1071と、利用者の認証を行う認証手段1091と、各手段を制御する実行制御手段1101とを備える。



### 【特許請求の範囲】

【請求項1】ネットワークを介し、特定の利用者を対象にアプリケーションサービスを提供するアプリケーションサーバと、利用者が送信する情報を出力しアプリケーションサーバが提供する情報を入力する利用者端末とが接続されたコンピュータシステムにおいて、ネットワークを介しアプリケーションサーバとの通信を行う対サーバ通信手段と、利用者端末との通信を行う対端末通信手段と、利用者の個人情報を格納するデータベースと、前記データベースに対して個人情報の検索、登録、変更、削除を含む操作を行うデータベース管理手段と、利用者の認証を行う認証手段と、前記各手段を制御する実行制御手段とを備え、利用者の認証により個人情報に基づき得られた認証情報をアプリケーションサーバに対する送信データに付加することを特徴とする個人情報管理装置。

【請求項2】各アプリケーションサービスに固有の利用者の権限情報や利用者とアプリケーションサーバとの通信メッセージを含むアプリケーション固有情報と、アプリケーション固有情報を利用者の個人情報と対応づけて管理する固有情報管理手段と、対応する利用者の固有情報をアプリケーションサーバに対し送受信する固有情報通信手段とを備え、アプリケーション固有情報を利用者の固有情報と対応づけて管理するようにしたことを特徴とする請求項1記載の個人情報管理装置。

【請求項3】複数の利用者のグループを特定する情報で構成されるグループ情報と、利用者の範囲を特定する条件に基いてグループを決定する利用者グループ決定手段とを備え、新たな利用者の登録があった際にグループ情報を作成または更新することを特徴とする請求項1または2記載の個人情報管理装置。

【請求項4】前記アプリケーション固有情報に含まれているアプリケーションサーバと利用者との送受信メッセージと送受信が行われた日時とから利用者が周期的に繰り返し送受信するメッセージの特徴を抽出するアプリケーション固有情報特徴抽出手段と、前記メッセージの特徴と現在時刻とを対応づけて利用者が次に要求する情報を予測する要求予測手段とを備え、アプリケーション固有情報から利用者が周期的に繰り返し送受信するメッセージの特徴を抽出し、時刻を対応づけて利用者が次に要求する情報を予測するようにしたことを特徴とする請求項1、2または3記載の個人情報管理装置。

【請求項5】ネットワーク上に配置された他の個人情報管理装置との通信を行う対個人情報管理装置通信手段と、個人情報管理装置のネットワークアドレスを管理するアドレステーブルと、必要に応じて他の個人情報管理装置に対し個人情報の検索を要求する一元情報検索手段とを備え、利用者からの接続要求に対し必要に応じて他の個人情報管理装置に対し個人情報の検索を要求するようにしたことを特徴とする請求項1、2、3または4記

載の個人情報管理装置。

【請求項6】データベースの内容を確認して個人情報やグループ情報を修正するメンテナンスを行うメンテナンス実行手段を備え、利用者が接続していない場合にデータベースの内容を自動的に確認して、個人情報やグループ情報を修正するメンテナンスを行うようにしたこと特徴とする請求項1、2、3、4または5記載の個人情報管理装置。

【請求項7】前記データベース管理手段は利用者に関するグループ情報を検索する機能およびグループ情報に対して登録、変更、削除などの操作を行う機能を含み、前記個人情報管理装置は個人情報の更新を検出する個人情報更新検出手段を備え、個人情報を更新した際に関係のあるグループ情報を自動的に更新するようにしたことを特徴とする請求項1、2、3、4、5または6記載の個人情報管理装置。

【請求項8】個人情報管理装置を起動して処理を開始し、利用者端末からの接続要求の受信を監視し、接続要求を受信するとデータベースから該当する利用者の個人情報を取得して認証を行い、認証に成功した場合は利用者に対応する子プロセスを起動し、起動された子プロセスは処理を開始して対端末通信手段及び対サーバ通信手段におけるデータ受信を監視し、データを受信すると送信先を確認し、アプリケーションサーバへの送信データであれば認証情報を付加して対サーバ通信手段から送信し、利用者端末に対する送信データであれば対端末通信手段から送信する各工程からなることを特徴とする個人情報管理方法。

### 【発明の詳細な説明】

#### 【0001】

【発明の属する技術分野】本発明は、特定の利用者を対象にアプリケーションサービスを提供する複数のアプリケーションサーバと利用者が操作を行う利用者端末がネットワークにより接続されたコンピュータシステムにおいて、特に個人情報を管理しアプリケーションサーバと利用者端末との情報授受を支援する個人情報管理装置に関する。

#### 【0002】

【従来の技術】従来、アプリケーションサービスの内容や処理手順を制御するアプリケーションサーバと利用者に対して情報を表示したり利用者から情報を受取る利用者端末とがネットワークに接続されたコンピュータシステムの特定の利用者に対してアプリケーションサービスを提供する場合、利用者は使用したいアプリケーションサービスを提供しているアプリケーションサーバに接続しなければならない。その際、利用者のアカウント、パスワード、性別、生年月日、所属などの個人情報がアプリケーションサーバ毎に管理されており、利用者が複数のアプリケーションサーバを使用する場合には、使用するアプリケーションサーバ毎に個人情報を送信する必

要があった。

#### 【0003】

【発明が解決しようとする課題】しかしながら、上記従来のアプリケーションサーバ毎に個人情報を管理する方法では、使用する複数のアプリケーションサーバへの個人情報の送信による利用者の操作負担の増加や、個人情報が複数の場所に保存されることによる資源の冗長利用や個人情報の不整合が生じる場合があるという問題があった。

【0004】本発明は、複数のアプリケーションサーバに対して使用する個人情報を一元的に管理して、アプリケーションサーバ毎に送信しなければならないような利用者の操作負担を軽減することを目的とする。

#### 【0005】

【課題を解決するための手段】本発明は、上記の課題を解決するため、特定の利用者を対象にアプリケーションサービスを提供するアプリケーションサーバと利用者が送信すべき情報の出力やアプリケーションサーバが提供する情報の入力を行う利用者端末との間に設けられた個人情報管理装置であって、個人情報管理装置はネットワークを介してアプリケーションサーバとの間の通信を行う対サーバ通信手段と、利用者端末との間の通信を行う対端末通信手段と、利用者のアカウント、パスワード、性別、生年月日、所属などで構成される個人情報を格納するデータベースと、データベースに対して個人情報の検索、登録、変更、削除などの操作を行うデータベース管理手段と、利用者の認証を行う認証手段と、アプリケーションサービスに固有の権限情報などで構成されるアプリケーション固有情報を利用者の個人情報と対応づけて管理する固有情報管理手段と、対応する利用者の固有情報をアプリケーションサーバに対し送受信する固有情報通信手段とを備え、アプリケーション固有情報を利用者の個人情報と対応づけて管理するようにしたものであり、個々のアプリケーションサービスに固有のアプリケーション固有情報を利用者の個人情報と対応づけて管理するようにしたことにより、利用者と個々のアプリケーションサーバとの間の固有の操作を軽減することができるという作用を有する。

【0006】本発明は、個人情報管理装置が管理するデータベースに格納した利用者の個人情報を複数のアプリケーションサーバが参照し、利用者は一度の認証処理で複数のアプリケーションサーバを利用することが可能となり、各種操作や処理を軽減することができる個人情報管理装置が得られる。

#### 【0007】

【発明の実施の形態】本発明の請求項1に記載の発明は、ネットワークを介し、特定の利用者を対象にアプリケーションサービスを提供するアプリケーションサーバと、利用者が送信する情報を出力しアプリケーションサーバが提供する情報を入力する利用者端末とが接続されたコンピュータシステムにおいて、ネットワークを介しアプリケーションサーバとの通信を行う対サーバ通信手段と、利用者端末との通信を行う対端末通信手段と、利用者の個人情報を格納するデータベースと、前記データ

ベースに対して個人情報の検索、登録、変更、削除を含む操作を行うデータベース管理手段と、利用者の認証を行う認証手段と、前記各手段を制御する実行制御手段とを備え、利用者の認証により個人情報に基づき得られた認証情報をアプリケーションサーバに対する送信データに付加するようにしたものであり、複数のアプリケーションサービスを利用する場合に、一度認証を行うことのみでアプリケーションサーバ毎に認証処理を行う必要がなく、認証処理を軽減することができるという作用を有する。

【0008】本発明の請求項2に記載の発明は、各アプリケーションサービスに固有の利用者の権限情報や利用者とアプリケーションサーバとの通信メッセージを含むアプリケーション固有情報と、アプリケーション固有情報を利用者の個人情報と対応づけて管理する固有情報管理手段と、対応する利用者の固有情報をアプリケーションサーバに対し送受信する固有情報通信手段とを備え、アプリケーション固有情報を利用者の固有情報を対応づけて管理するようにしたものであり、個々のアプリケーションサービスに固有のアプリケーション固有情報を利用者の固有情報を対応づけて管理するようにしたことにより、利用者と個々のアプリケーションサーバとの間の固有の操作を軽減することができるという作用を有する。

【0009】本発明の請求項3に記載の発明は、複数の利用者のグループを特定する情報で構成されるグループ情報と、利用者の範囲を特定する条件に基いてグループを決定する利用者グループ決定手段とを備え、新たな利用者の登録があった際にグループ情報を作成または更新するようにしたものであり、グループを対象に情報提供を行う際、情報を配信したい複数の利用者を選別する処理を軽減することができるという作用を有する。

【0010】本発明の請求項4に記載の発明は、前記アプリケーション固有情報に含まれているアプリケーションサーバと利用者との送受信メッセージと送受信が行われた日時とから利用者が周期的に繰り返し送受信するメッセージの特徴を抽出するアプリケーション固有情報特徴抽出手段と、前記メッセージの特徴と現在時刻とを対応づけて利用者が次に要求する情報を予測する要求予測手段とを備え、アプリケーション固有情報から利用者が周期的に繰り返し送受信するメッセージの特徴を抽出し、時刻を対応づけて利用者が次に要求する情報を予測するようにしたものであり、アプリケーション固有情報から利用者が周期的に繰り返し送受信するメッセージの特徴を抽出したものに、送受信した時刻を対応づけて利用者が次に要求する情報を予測するようにしたことにより、要求される情報を利用者の操作に先行して受信し利用者の応答待ち時間を短縮することができるという作用を有する。

【0011】本発明の請求項5に記載の発明は、ネット

ワーク上に配置された他の個人情報管理装置との通信を行う対個人情報管理装置通信手段と、個人情報管理装置のネットワークアドレスを管理するアドレステーブルと、必要に応じて他の個人情報管理装置に対し個人情報の検索を要求する一元情報検索手段とを備え、利用者からの接続要求に対し必要に応じて他の個人情報管理装置に対し個人情報の検索を要求するようにしたものであり、利用者からの接続要求を受信した際に、必要に応じ、自動的に他の個人情報管理装置に対し個人情報の検索を要求するようにしたことにより、利用者は自己の個人情報の格納先を意識することなく任意の個人情報管理装置に接続することができるという作用を有する。

【0012】本発明の請求項6に記載の発明は、データベースの内容を確認して個人情報やグループ情報を修正するメンテナンスを行うメンテナンス実行手段を備え、利用者が接続していない場合にデータベースの内容を自動的に確認して、個人情報やグループ情報を修正するメンテナンスを行うようにしたものであり、利用者が接続していない場合などにデータベースの内容を自動的に確認して、個人情報やグループ情報の重複登録や矛盾等の修正のようなメンテナンスを定期的または自動的に行うことにより、管理者によるメンテナンス操作の軽減を図ることができるという作用を有する。

【0013】本発明の請求項7に記載の発明は、前記データベース管理手段が利用者に関するグループ情報を検索する機能およびグループ情報に対して登録、変更、削除などの操作を行う機能を含み、前記個人情報管理装置は個人情報の更新を検出する個人情報更新検出手段を備え、個人情報を更新した際に関係のあるグループ情報を自動的に更新するようにしたものであり、個人情報を更新した際に関係のあるグループ情報を自動的に更新することができるようによることにより、メンテナンス操作の軽減を図ることができるという作用を有する。

【0014】本発明の請求項8に記載の発明は、個人情報管理装置を起動して処理を開始し、利用者端末からの接続要求の受信を監視し、接続要求を受信するとデータベースから該当する利用者の個人情報を取得して認証を行い、認証に成功した場合は利用者に対応する子プロセスを起動し、起動された子プロセスは処理を開始して対端末通信手段及び対サーバ通信手段におけるデータ受信を監視し、データを受信すると送信先を確認し、アプリケーションサーバへの送信データであれば認証情報を附加して対サーバ通信手段から送信し、利用者端末に対する送信データであれば対端末通信手段から送信するようにしたものであり、複数のアプリケーションサービスを利用する場合に、一度認証を行うことのみでアプリケーションサーバ毎に認証処理を行う必要がなく、認証処理を軽減することができるという作用を有する。

【0015】以下、添付図面、図1乃至図14に基づき、本発明の第1乃至第7の実施の形態を詳細に説明す

る。

（第1の実施の形態）本発明の第1の実施の形態における個人情報管理装置は、ネットワークを介してアプリケーションサーバとの通信を行う対サーバ通信手段と、利用者端末との通信を行う対端末通信手段と、データベースと、データベース管理手段と、認証手段と、これらの実行制御を行う実行制御手段とを備え、利用者端末を介して接続された利用者の認証を行うことにより得られた認証情報をアプリケーションサーバに対するデータ送信時に付加することにより、各々のアプリケーションサーバとの認証処理を省略して利用者の認証操作の負担を軽減することができるものである。

【0016】まず、図1を参照して、本発明の第1の実施の形態における個人情報管理装置の構成を説明する。図1は本発明の第1の実施の形態における個人情報管理装置の構成を示すブロック図である。図1において、1011～1012は特定の利用者を対象にアプリケーションサービスを提供するアプリケーションサーバである。1021は個人情報を格納するデータベースである。1031は利用者が送信すべき情報の出力とアプリケーションサーバ1011～1012が提供する情報の入力を行う利用者端末である。1041は個人情報管理装置であり、対サーバ通信手段1051と、対端末通信手段1061と、データベース管理手段1071と、個人情報1081と、認証手段1091と、実行制御手段1101とからなる。

【0017】対サーバ通信手段1051はネットワークを介してアプリケーションサーバ1011、1012との通信を行う手段である。対端末通信手段1061は同様にネットワークを介して利用者端末1031との通信を行う手段である。データベース管理手段1071はデータベース1021に対して個人情報の検索、登録、変更、削除などの操作を行う手段である。個人情報1081は利用者のアカウント、パスワード、性別、生年月日、所属などで構成される情報である。認証手段1091は、利用者端末1031と対端末通信手段1061を介して得られた利用者のアカウントおよびパスワードと、データベースから取得した個人情報1081を用いて認証を行う手段である。実行制御手段1101は対サーバ通信手段1051、対端末通信手段1061、データベース管理手段1071、認証手段1091の実行を制御し、利用者端末1031からの認証データとデータベースから取得した個人情報1081を用いて認証を行い、認証が成功した場合には利用者端末1031及びアプリケーションサーバ1011、1012からの受信データの配信を行う。

【0018】次に、図2を参照して、本発明の第1の実施の形態における個人情報管理装置の動作を説明する。図2は図1に示す本発明の第1の実施の形態における個人情報管理装置の処理の流れを示すフローチャートであ

る。なお、図2中、201、202、・・・、258は処理手順の番号を示す。図2において、ステップ201から207は管理装置本体の処理フローであり、ステップ251から258はステップ205において、各利用者に対応づけて起動される子プロセスの処理フローである。まず、個人情報管理装置1041が起動すると、実行制御手段1101が処理を開始し（ステップ201）、対端末通信手段1061が利用者端末1031からの接続要求の受信を監視する（ステップ202）。接続要求を受信すると、データベース管理手段1071を用いてデータベース1021から該当する利用者の個人情報1081を取得し（ステップ203）、認証手段1091により認証を行う（ステップ204）。

【0019】認証に失敗した場合にはその旨を利用者に通知し（ステップ206）、対端末通信手段1061と利用者端末1031との通信を切断する（ステップ207）。認証に成功した場合は、利用者に対応する子プロセスを起動して子プロセスに対し個人情報1081渡す（ステップ205）。起動された子プロセスは処理を開始し（ステップ251）、対端末通信手段1061と対サーバ通信手段1051におけるデータ受信を監視する（ステップ252）。データを受信した場合は、送信先を確認し（ステップ253）、アプリケーションサーバ1011～1012への送信データであれば認証情報を付加して対サーバ通信手段1051から送信する（ステップ254）。また、利用者端末1031に対する送信データであれば対端末通信手段1061から送信する（ステップ255）。

【0020】次に、利用者端末1031との接続状況を確認し（ステップ256）、接続されている場合にはデータ通信処理（ステップ252～256）を繰り返し実行する。利用者端末1031との接続が切断された場合には、データベース管理手段1071により個人情報をデータベースに保存して（ステップ257）処理を終了する（ステップ258）。

【0021】上記のように、本発明の第1の実施の形態においては、個人情報管理装置が、対サーバ通信手段と、対端末通信手段と、データベース管理手段と、認証手段と、実行制御手段とを備え、アプリケーションサーバへの送信データに個人情報に基づいた認証情報を付加するよう構成したので、個々のアプリケーションサーバに対する認証処理を省略することが可能となる。

【0022】（第2の実施の形態）本発明の第2の実施の形態における個人情報管理装置は、対サーバ通信手段と、対端末通信手段と、データベースと、データベース管理手段と、認証手段と、固有情報管理手段と、固有情報通信手段と、実行制御手段とを備え、アプリケーションサービスに固有のアプリケーション固有情報を利用者の個人情報と対応づけて管理することにより、利用者とアプリケーションサーバとの間の固有な操作の軽減を可

能にするものである。

【0023】まず、図3を参照して、本発明の第2の実施の形態における個人情報管理装置の構成を説明する。図3は本発明の第2の実施の形態における個人情報管理装置の構成を示すブロック図である。図3において、3011～3013は特定の利用者を対象にアプリケーションサービスを提供するアプリケーションサーバである。3021は個人情報や後述のアプリケーション固有情報を格納するデータベースである。3031は利用者が送信すべき情報の出力とアプリケーションサーバ3011～3013が提供する情報の入力を行う利用者端末である。3041個人情報管理装置であり、対サーバ通信手段3051と、対端末通信手段3061と、データベース管理手段3071と、個人情報3081と、認証手段3091と、実行制御手段3101と、個有情報管理手段3111と、アプリケーション固有情報3121と、固有情報通信手段3131とからなる。

【0024】対サーバ通信手段3051は、ネットワークを介してアプリケーションサーバとの通信を行う手段である。対端末通信手段3061は、同様にネットワークを介して利用者端末との通信を行う手段である。データベース管理手段3071は、データベースに対して個人情報やアプリケーション固有情報の検索、登録、変更、削除などの操作を行う手段である。個人情報3081は、利用者のアカウント、パスワード、性別、生年月日、所属などで構成される情報である。認証手段3091は、利用者端末3031と対端末通信手段3061を介して得られた利用者のアカウントおよびパスワードと、データベースから取得した個人情報3081とを用いて認証を行う手段である。アプリケーション固有情報3121は、アプリケーションサービスにおける利用者の権限や、利用者とアプリケーションサーバとの通信メッセージの履歴などで構成される情報である。

【0025】固有情報管理手段3111は、アプリケーション固有情報3121と利用者の個人情報3081とを対応づけて管理する手段である。固有情報通信手段3131は、アプリケーションサーバ3011～3013との間でアプリケーション固有情報3121を通信する手段である。実行制御手段3101は、必要に応じ、固有情報通信手段3131を用いてアプリケーション固有情報3121を通信し、固有情報管理手段3111によって個人情報3081と対応づけ、対サーバ通信手段3051、対端末通信手段3061、データベース管理手段3071、認証手段3091の実行を制御する手段である。

【0026】次に、図4を参照して、本発明の第2の実施の形態における個人情報管理装置の動作を説明する。図4は図3に示す本発明の第2の実施の形態における個人情報管理装置の処理の流れを示すフローチャートである。なお、図4の処理フローは、図2に示す、第1の実

施の形態の処理フローとの相違点を説明するためのもので、図2のステップ205で起動される子プロセスの処理フローである。なお、図4中の451、452、・・・、460は処理手順の番号である。まず、図4の処理フローの理解を容易にするために、図2を参照してステップ201からステップ205に至るまでの処理フローを説明する。従って、図4の説明は、以下図2の説明から開始する。なお、図2の説明においては、図3の各構成部を使用するため、図3の構成部の符号を使用する。

【0027】まず、個人情報管理装置3041を起動すると、実行制御手段3101が処理を開始し（ステップ201）、対端末通信手段3061が利用者端末3031からの接続要求の受信を監視する（ステップ202）。接続要求を受信すると、データベース管理手段3071を用いてデータベース3021から該当する利用者の個人情報3081を取得し（ステップ203）、認証手段3091により認証を行う（ステップ204）。認証に失敗した場合にはその旨を利用者に通知し（ステップ206）、対端末通信手段3061と利用者端末3031との通信を切断する（ステップ207）。認証に成功した場合は、利用者に対する子プロセスを起動して個人情報3081を渡す（ステップ205）。

【0028】そこで、図4の処理フローに進み、起動された子プロセスは処理を開始し（ステップ451）、対端末通信手段3061と対サーバ通信手段3051におけるデータ受信を監視する（ステップ452）。データを受信した場合は、送信先を確認し（ステップ453）、アプリケーションサーバ3011～3013への送信データ（情報要求）であれば認証情報を付加して対サーバ通信手段3051により送信し（ステップ454）、アプリケーション固有情報の必要性を確認し（ステップ456）、必要な場合には固有情報通信手段3131が対サーバ通信手段3051を使用して送受信を行う（ステップ457）。

【0029】また、利用者端末3031に対する送信データであれば対端末通信手段3061により送信を行う（ステップ455）。次に利用者端末3031との接続状況を確認し（ステップ458）、接続されている場合にはデータ通信処理（ステップ452～458）を繰り返し実行する。利用者端末3031との接続が切断された場合には、データベース管理手段3071により個人情報をデータベース3021に保存して（ステップ459）処理を終了する（ステップ460）。

【0030】上記のように、本発明の第2の実施の形態においては、個人情報管理装置が、対サーバ通信手段と、対端末通信手段と、データベース管理手段と、認証手段と、固有情報管理手段と、固有情報通信手段と、実行制御手段とを備え、アプリケーションサービスに固有である利用者の権限や、送受信データの履歴などで構成されるアプリケーション固有情報を利用者の個人情報と

対応づけて管理するよう構成したので、利用者とアプリケーションサーバとの固有な操作の軽減が可能となる。

【0031】（第3の実施の形態）本発明の第3の実施の形態における個人情報管理装置は、対サーバ通信手段と、対端末通信手段と、データベースと、データベース管理手段と、認証手段と、固有情報管理手段と、固有情報通信手段と、利用者グループ決定手段と、実行制御手段とを備え、複数の利用者の集合である利用者グループを性別や年齢などの条件に基いて決定することにより、複数の利用者に対して情報提供を行う場合に該当する利用者を選別する処理を軽減することができるものである。

【0032】まず、図5を参照して、本発明の第3の実施の形態における個人情報管理装置の構成を説明する。図5は本発明の第3の実施の形態における個人情報管理装置の構成を示すブロック図である。図5において、5011～5013は特定の利用者を対象にアプリケーションサービスを提供するアプリケーションサーバである。5021は個人情報やアプリケーション固有情報、および後述のグループ情報を格納するデータベースである。5031は利用者が送信すべき情報の出力とアプリケーションサーバ5011～5013が提供する情報の入力を行う利用者端末である。5041は個人情報管理装置であり、対サーバ通信手段5051と、対端末通信手段5061と、データベース管理手段5071と、個人情報5081と、認証手段5091と、実行制御手段5101と、固有情報管理手段5111と、アプリケーション固有情報5121と、固有情報通信手段5131と、利用者グループ決定手段5141と、グループ情報5151とからなる。

【0033】対サーバ通信手段5051は、ネットワークを介してアプリケーションサーバ5011～5013との通信を行う手段である。対端末通信手段5061は、同様にネットワークを介して利用者端末5031との通信を行う手段である。データベース管理手段5071は、データベース5021に対して個人情報5081やアプリケーション固有情報5121、およびグループ情報5151の検索、登録、変更、削除などの操作を行う手段である。

【0034】個人情報5081は、利用者のアカウント、パスワード、性別、生年月日、所属などで構成される情報である。認証手段5091は、利用者端末と対端末通信手段を介して得られた利用者のアカウントおよびパスワードと、データベースから取得した個人情報を用いて認証を行う手段である。アプリケーション固有情報5121は、アプリケーションサービスにおける利用者の権限や、送受信データの履歴などで構成される情報である。固有情報管理手段5111は、アプリケーション固有情報と利用者の個人情報を対応づけて管理する手段である。固有情報通信手段5131は、アプリケーション

ンサーバとの間でアプリケーション固有情報を通信する手段である。

【0035】利用者グループ決定手段5141は、性別や年齢など利用者の範囲を特定する条件に該当する複数の利用者を決定する手段である。グループ情報5151は、名称、コード、管理者、条件、該当利用者などで構成されるグループを特定する情報である。実行制御手段5101は、必要に応じて利用者グループに対してアプリケーションサーバ5011～5013からの情報を提供するため、利用者グループ決定手段5141を用いてグループ情報5151を作成し、対サーバ通信手段5051、対端末通信手段5061、データベース管理手段5071、認証手段5091、固有情報管理手段5111の実行を制御する手段である。

【0036】次に、図6を参照して、本発明の第3の実施の形態における個人情報管理装置の動作を説明する。図6は図5に示す本発明の第3の実施の形態における個人情報管理装置の処理の流れを示すフローチャートである。なお、図6中の601、602、・・・、611は処理手順の番号であり、個人情報管理装置5041が起動すると、実行制御手段5101が処理を開始し（ステップ601）、対端末通信手段5061が利用者端末5031からの接続要求の受信を監視する（ステップ602）。接続要求を受信すると、データベース管理手段5071を用いてデータベース5021から該当する利用者の個人情報を取得し（ステップ603）、認証手段5091により認証を行う（ステップ604）。

【0037】認証に失敗した場合にはその旨を利用者に通知し（ステップ606）、対端末通信手段5061と利用者端末5031との通信を切断する（ステップ607）。認証に成功した場合は、利用者に対応する子プロセスを起動して個人情報5081を渡す（ステップ605）。実行制御手段5101はグループの作成が必要かどうかを判断するため、利用者の新規登録状況を確認する（ステップ608）。グループの作成が必要な場合には、利用者グループ決定手段5141がデータベース5021からグループ情報を取得し（ステップ609）、個人情報を検索してグループ情報5151を作成または更新する（ステップ610）。

【0038】次に、データベース管理手段5071は、作成または更新されたグループ情報5151をデータベース5021に保存し（ステップ611）、接続要求の監視を再開する。グループの作成が必要ない場合には、これらの処理を行わずに、接続要求の監視に戻る。

【0039】上記のように、本発明の第3の実施の形態においては、個人情報管理装置が、対サーバ通信手段と、対端末通信手段と、データベース管理手段と、認証手段と、固有情報管理手段と、固有情報通信手段と、利用者グループ決定手段と、実行制御手段とを備え、新たな利用者の登録があった際にグループ情報を作成または

更新するよう構成したので、情報を配信したい複数の利用者を選別する処理を軽減することができる。

【0040】（第4の実施の形態）本発明の第4の実施の形態における個人情報管理装置は、対サーバ通信手段と、対端末通信手段と、データベースと、データベース管理手段と、認証手段と、固有情報管理手段と、固有情報通信手段と、利用者グループ決定手段と、固有情報特徴抽出手段と、要求予測手段と、実行制御手段とを備え、アプリケーション固有情報から利用者が周期的に繰り返し送受信するメッセージの特徴を抽出し、時刻を対応づけて利用者が次に要求する情報を予測することにより、予測した情報を利用者の操作に先行して受信し利用者の応答待ち時間を軽減することを可能にするものである。

【0041】まず、図7を参照して、本発明の第4の実施の形態における個人情報管理装置の構成を説明する。図7は本発明の第4の実施の形態における個人情報管理装置の構成を示すブロック図である。図7において、7011～7013は特定の利用者を対象にアプリケーションサービスを提供するアプリケーションサーバである。7021は個人情報やアプリケーション固有情報、およびグループ情報を格納するデータベースである。7031は利用者が送信すべき情報の出力とアプリケーションサーバ7011～7013が提供する情報の入力をを行う利用者端末である。7041は個人情報管理装置であり、対サーバ通信手段7051と、対端末通信手段7061と、データベース管理手段7071と、個人情報7081と、認証手段7091と、実行制御手段7101と、固有情報管理手段7111と、アプリケーション固有情報7121と、固有情報通信手段7131と、利用者グループ決定手段7141と、グループ情報7151と、固有情報特徴抽出手段7161と、要求予測手段7171と、バッファ7181とからなる。

【0042】対サーバ通信手段7051は、ネットワークを介してアプリケーションサーバ7011～7013との通信を行う手段である。対端末通信手段7061は、同様にネットワークを介して利用者端末7031との通信を行う手段である。データベース管理手段7071は、データベース7071に対して個人情報7081やアプリケーション固有情報7121およびグループ情報7151の検索、登録、変更、削除などの操作を行う手段である。個人情報7081は、利用者のアカウント、パスワード、性別、生年月日、所属などで構成される情報である。認証手段7091は、利用者端末と対端末通信手段を介して得られた利用者のアカウントおよびパスワードとデータベースから取得した個人情報7081とを用いて認証を行う手段である。

【0043】アプリケーション固有情報7121は、アプリケーションサービスにおける利用者の権限や、送受信データの履歴などで構成される情報である。固有情報

管理手段 7111 は、アプリケーション固有情報 7121 と利用者の個人情報 7081 を対応づけて管理する手段である。固有情報通信手段 7131 は、アプリケーションサーバ 7011～7013 との間でアプリケーション固有情報 7121 を通信する手段である。利用者グループ決定手段 7141 は、性別や年齢などの条件に該当する複数の利用者を決定する手段である。グループ情報 7151 は、名称、コード、管理者、条件、該当利用者などで構成される情報である。固有情報特徴抽出手段 7161 は、アプリケーション固有情報 7121 から利用者が周期的に繰り返し送受信するメッセージの特徴を抽出する手段である。

【0044】要求予測手段 7171 は、時刻を対応づけて利用者が次に要求する情報を予測する手段である。実行制御手段 7101 は、利用者の要求を予測し先行して情報を受信し、受信した情報をバッファ 7181 に格納するよう、対サーバ通信手段 7051、対端末通信手段 7061、データベース管理手段 7071、認証手段 7091、固有情報管理手段 7111、固有情報通信手段 7131、利用者グループ決定手段 7141、固有情報特徴抽出手段 7161 の実行を制御する手段である。

【0045】次に、図 8 を参照して、本発明の第4の実施の形態における個人情報管理装置の動作を説明する。図 8 は図 7 に示す本発明の第4の実施の形態における個人情報管理装置の処理の流れを示すフローチャートである。なお、図 8 の処理フローは、図 6 に示す、第3の実施の形態の処理フローとの相違点を説明するためのもので、図 6 のステップ 605 で起動される子プロセスの処理フローである。なお、図 8 中の 851、852、・・・、862 は処理手順の番号である。まず、図 8 の処理フローの理解を容易にするために、図 6 を参照してステップ 601 からステップ 605 に至るまでの処理フローを説明する。従って、図 8 の説明は、以下図 6 の説明から開始する。なお、図 6 の説明においては、図 7 の各構成部を使用するため、図 7 の構成部の符号を使用する。

【0046】まず、個人情報管理装置 7041 を起動すると、実行制御手段 7101 が処理を開始し（ステップ 601）、対端末通信手段 7061 が利用者端末 7031 からの接続要求の受信を監視する（ステップ 602）。接続要求を受信すると、データベース管理手段 7071 を用いてデータベース 7021 から該当する利用者の個人情報 7081 を取得し（ステップ 603）、認証手段 7091 により認証を行う（ステップ 604）。認証に失敗した場合にはその旨を利用者に通知し（ステップ 606）、対端末通信手段 7061 と利用者端末 7031 との通信を切断する（ステップ 607）。認証に成功した場合は、利用者に対応する子プロセスを起動して個人情報 7081 を渡す（ステップ 605）。

【0047】そこで、図 8 の処理フローに進み、起動された子プロセスは処理を開始し（ステップ 851）、対

端末通信手段 7061 と対サーバ通信手段 7051 におけるデータ受信を監視する（ステップ 852）。データを受信した場合は、そのデータの送信先を確認し（ステップ 853）、アプリケーションサーバ 7011～7013 への送信データ（情報要求）であれば、バッファ 7181 に該当情報があるかどうかを確認し（ステップ 854）、あればそれを対端末通信手段 7061 によって送信する（ステップ 856）。該当情報がない場合は、認証情報を附加して対サーバ通信手段 7051 により送信し（ステップ 855）、アプリケーション固有情報の必要性を確認し（ステップ 857）、必要な場合には固有情報通信手段 7131 が対サーバ通信手段 7051 を使用して送受信を行う（ステップ 858）。また、利用者端末 7031 への送信データであれば対端末通信手段 7061 により送信する（ステップ 856）。

【0048】次に、時刻と固有情報に基づいて、要求予測手段 7171 が予測した要求によりアプリケーションサーバ 7011～7013 からデータを受信し、バッファ 7181 に格納する（ステップ 859）。利用者端末 7031 との接続状況を確認し（ステップ 860）、接続されている場合にはデータ受信処理（ステップ 852～860）を繰り返し実行する。利用者端末 7031 との接続が切断された場合には、データベース管理手段 7071 により個人情報をデータベース 7021 に保存し（ステップ 861）処理を終了する（ステップ 862）。

【0049】上記のように、本発明の第4の実施の形態においては、個人情報管理装置が、対サーバ通信手段と、対端末通信手段と、データベースと、データベース管理手段と、認証手段と、固有情報管理手段と、固有情報通信手段と、利用者グループ決定手段と、固有情報特徴抽出手段と、要求予測手段と、実行制御手段とを備え、アプリケーション固有情報から利用者が周期的に繰り返し送受信するメッセージの特徴を抽出し、時刻を対応づけて利用者が次に要求する情報を予測するよう構成したので、要求される情報を利用者の操作に先行して受信し利用者の応答待ち時間を軽減することができる。

【0050】（第5の実施の形態）本発明の第5の実施の形態における個人情報管理装置は、対サーバ通信手段と、対端末通信手段と、データベースと、データベース管理手段と、認証手段と、固有情報管理手段と、固有情報通信手段と、利用者グループ決定手段と、固有情報特徴抽出手段と、要求予測手段と、一元情報検索手段と、対個人情報管理装置通信手段と、実行制御手段とを備え、利用者からの接続要求を受信した際に、必要に応じて他の個人情報管理装置に対し個人情報の検索を要求することによって、利用者が自己の個人情報の格納先を意識せずに任意の個人情報管理装置に接続することができ、移動した利用者が異なる利用者端末から接続した場合でも、同一のアプリケーションサービスを受けること

ができる分散型の個人情報管理装置である。

【0051】まず、図9を参照して、本発明の第5の実施の形態における個人情報管理装置の構成を説明する。図9は本発明の第5の実施の形態における個人情報管理装置の構成を示すブロック図である。図9において、9011～9013は特定の利用者を対象にアプリケーションサービスを提供するアプリケーションサーバである。9021は個人情報やアプリケーション固有情報およびグループ情報を格納するデータベースである。9031は利用者が送信すべき情報の出力とアプリケーションサーバ9011～9013が提供する情報の入力をを行う利用者端末である。9041は個人情報管理装置であり、対サーバ通信手段9051と、対端末通信手段9061と、データベース管理手段9071と、個人情報9081と、認証手段9091と、実行制御手段9101と、固有情報管理手段9111と、アプリケーション固有情報9121と、固有情報通信手段9131と、利用者グループ決定手段9141と、グループ情報9151と、固有情報特徴抽出手段9161と、要求予測手段9171と、バッファ9181と、一元情報検索手段9191と、対個人情報管理装置通信手段9201とからなる。

【0052】対サーバ通信手段9051は、ネットワークを介してアプリケーションサーバ9011～9013との通信を行う手段である。対端末通信手段9061は、同様にネットワークを介して利用者端末9031との通信を行う手段である。データベース管理手段9071は、データベース9021に対して個人情報9081やアプリケーション固有情報9121、およびグループ情報9151の検索、登録、変更、削除などの操作を行う手段である。個人情報9081は、利用者のアカウント、パスワード、性別、生年月日、所属などで構成される情報である。認証手段9091は、利用者端末9031と対端末通信手段9061を介して得られた利用者のアカウントおよびパスワードと、データベース9021から取得した個人情報9081を用いて認証を行う手段である。

【0053】アプリケーション固有情報9121は、アプリケーションサービスにおける利用者の権限や、送受信データの履歴などで構成される情報である。固有情報管理手段9111は、アプリケーション固有情報9121と利用者の個人情報9081とを対応づけて管理する手段である。固有情報通信手段9131は、アプリケーションサーバ9011～9013との間でアプリケーション固有情報9121を通信する手段である。利用者グループ決定手段9141は、性別や年齢などの条件に該当する複数の利用者を決定する手段である。グループ情報9151は、名称、コード、管理者、条件、該当利用者などで構成される情報である。

【0054】また、固有情報特徴抽出手段9161は、

アプリケーション固有情報9121から利用者が周期的に繰り返し送受信するメッセージの特徴を抽出する手段である。要求予測手段9171は、時刻を対応づけて利用者が次に要求する情報を予測する手段である。一元情報検索手段9191は、例えば、自己のデータベース9021に求める個人情報9081が存在しない場合など、必要に応じてネットワークに接続された他の個人情報管理装置9221～9222に対し個人情報の検索を要求するため、そのネットワークアドレスを格納したアドレステーブル9211を管理して一元的な情報検索を行う手段である。対個人情報管理装置通信手段9201は、ネットワークを介して他の個人情報管理装置9221～9222との通信を行う手段である。

【0055】実行制御手段9101は、利用者からの接続要求を受信した際に、自己のデータベースに該当する個人情報が存在しない場合に、他の個人情報管理装置9221～9222に対して個人情報を検索するよう、対サーバ通信手段9051、対端末通信手段9061、データベース管理手段9071、認証手段9091、固有情報管理手段9111、固有情報通信手段9131、利用者グループ決定手段9141、固有情報特徴抽出手段9161、要求予測手段9171、一元情報検索手段9191、対個人情報管理装置通信手段9201の実行を制御する手段である。

【0056】次に、図10を参照して、本発明の第5の実施の形態における個人情報管理装置の動作を説明する。図10は図9に示す本発明の第5の実施の形態における個人情報管理装置の処理の流れを示すフローチャートである。なお、図10中の1001、1002、…、1013は処理手順の番号である。まず、個人情報管理装置9041が起動すると、実行制御手段9101が処理を開始し（ステップ1001）、対端末通信手段9061が利用者端末9031からの接続要求を受信を監視する（ステップ1002）。接続要求を受信すると、データベース管理手段9071を用いてデータベース9021から該当する利用者の個人情報を検索し（ステップ1003）、結果を確認する（ステップ1004）。該当する個人情報9081が存在しない場合には、一元情報検索手段9191により、アドレステーブル9211に登録されている他の個人情報管理装置9221～9222に対して、対個人情報管理装置通信手段9201を介して個人情報9081の検索を要求する（ステップ1005）。

【0057】次に、認証手段9091により認証を行う（ステップ1006）。認証に失敗した場合にはその旨を利用者に通知し（ステップ1008）、対端末通信手段9061と利用者端末9031との通信を切断する（ステップ1009）。認証に成功した場合は、利用者に対応する子プロセスを起動して個人情報9081を渡す（ステップ1007）。実行制御手段9101はグル

ープの作成が必要か判断するため、利用者の新規登録状況を確認する（ステップ1010）。グループの作成が必要な場合には、利用者グループ決定手段9141がデータベース9021からグループ情報を取得し（ステップ1011）、個人情報9081を検索してグループ情報9151を作成または更新する（ステップ1012）。

【0058】次に、データベース管理手段9071により、作成または更新されたグループ情報9151をデータベース9021に保存し（ステップ1013）、接続要求の監視を再開する。グループの作成が必要ない場合には、これらの処理を行わずに、接続要求の監視に戻る。

【0059】上記のように、本発明の第5の実施の形態においては、個人情報管理装置が、対サーバ通信手段と、対端末通信手段と、データベース管理手段と、認証手段と、固有情報管理手段と、固有情報通信手段と、利用者グループ決定手段と、一元情報検索手段と、対個人情報管理装置通信手段と、実行制御手段とを備え、利用者からの接続要求を受信した際に、必要に応じて他の個人情報管理装置に対し個人情報の検索を要求することによって、利用者が自己の個人情報の格納先を意識することなく、任意の個人情報管理装置に接続できるよう構成したので、移動した利用者が異なる利用者端末から接続した場合でも同一のアプリケーションサービスを受けることが可能となる。

【0060】（第6の実施の形態）本発明の第6の実施の形態における個人情報管理装置は、対サーバ通信手段と、対端末通信手段と、データベースと、データベース管理手段と、認証手段と、固有情報管理手段と、固有情報通信手段と、利用者グループ決定手段と、固有情報特徴抽出手段と、要求予測手段と、一元情報検索手段と、対個人情報管理装置通信手段と、メンテナンス実行手段と、実行制御手段とを備え、データベースに管理する情報の重複保存の防止などのためのメンテナンスを定期的または自動的に実行することにより、管理者によるメンテナンス操作を軽減することを可能にする分散型の個人情報管理装置である。

【0061】まず、図11を参照して、本発明の第6の実施の形態における個人情報管理装置の構成を説明する。図11は本発明の第6の実施の形態における個人情報管理装置の構成を示すブロック図である。図11において、11011～11013は特定の利用者を対象にアプリケーションサービスを提供するアプリケーションサーバである。11021は個人情報やアプリケーション固有情報、およびグループ情報を格納するデータベースである。11031は利用者が送信すべき情報の出力とアプリケーションサーバ11011～11013が提供する情報の入力を行う利用者端末である。

【0062】また、11041は個人情報管理装置であ

り、対サーバ通信手段11051と、対端末通信手段11061と、データベース管理手段11071と、個人情報11081と、認証手段11091と、実行制御手段11101と、固有情報管理手段11111と、アプリケーション固有情報11121と、固有情報通信手段11131と、利用者グループ決定手段11141と、グループ情報11151と、固有情報特徴抽出手段11161と、要求予測手段11171と、バッファ11181と、一元情報検索手段11191と、対個人情報管理装置通信手段11201と、アドレステーブル11211と、メンテナンス実行手段11231とからなる。

【0063】対サーバ通信手段11051は、ネットワークを介してアプリケーションサーバとの通信を行う手段である。対端末通信手段11061は、同様にネットワークを介して利用者端末11031との通信を行う手段である。データベース管理手段11071は、データベース11021に対して個人情報11081やアプリケーション固有情報11121、およびグループ情報11151の検索、登録、変更、削除などの操作を行う手段である。個人情報11081は、利用者のアカウント、パスワード、性別、生年月日、所属などで構成される情報である。認証手段11091は、利用者端末11031と対端末通信手段11061を介して得られた利用者のアカウントおよびパスワードと、データベース11021から取得した個人情報11081を用いて認証を行う手段である。

【0064】アプリケーション固有情報11121は、アプリケーションサービスにおける利用者の権限や、送受信データの履歴などで構成される情報である。固有情報管理手段11111は、アプリケーション固有情報11121と利用者の個人情報11081とを対応づけて管理する手段である。固有情報通信手段11131は、アプリケーションサーバ11011～11013との間でアプリケーション固有情報11121を通信する手段である。

【0065】利用者グループ決定手段11141は、性別や年齢など利用者の範囲を特定する条件に該当する複数の利用者を決定する手段である。グループ情報11151は、名称、コード、管理者、条件、該当利用者などで構成される情報である。固有情報特徴抽出手段11161は、アプリケーション固有情報11121から利用者が周期的に繰り返し送受信するメッセージの特徴を抽出する手段である。要求予測手段11171は、時刻を対応づけて利用者が次に要求する情報を予測する手段である。

【0066】一元情報検索手段11191は、ネットワーク接続された他の個人情報管理装置11221～11222のネットワークアドレスを格納したアドレステーブル11211を管理し、一元的な情報検索を行う手段である。対個人情報管理装置通信手段11201は、ネ

ットワークを介して他の個人情報管理装置11221～11222との通信を行う手段である。メンテナンス実行手段11231は、データベース管理手段11071を通じてデータベース11021の内容を確認し、個人情報11081やグループ情報11151の重複登録や矛盾などをメンテナンスする手段である。実行制御手段11101は、利用者が接続していない場合などにメンテナンスを実行するよう、対サーバ通信手段11051、対端末通信手段11061、データベース管理手段11071、認証手段11091、固有情報管理手段11111、固有情報通信手段11131、利用者グループ決定手段11141、固有情報特徴抽出手段11161、要求予測手段11171、一元情報検索手段11191、対個人情報管理装置通信手段11201、メンテナンス実行手段11231の実行を制御する手段である。

【0067】次に、図12を参照して、本発明の第6の実施の形態における個人情報管理装置の動作を説明する。図12は図11に示す本発明の第6の実施の形態における個人情報管理装置の処理の流れを示すフローチャートである。なお、図12中の1201、1202、・・・、1215は処理手順の番号である。まず、個人情報管理装置11041が起動すると、実行制御手段11101が処理を開始し（ステップ1201）、対端末通信手段11061が利用者端末11031からの接続要求の受信を監視する（ステップ1202）。

【0068】接続要求を受信すると、データベース管理手段11071を用いてデータベース11021から該当する利用者の個人情報11081を検索し（ステップ1203）、結果を確認する（ステップ1204）。該当する個人情報11081が存在しない場合には、一元情報検索手段11191により、アドレステーブル11211に登録されている他の個人情報管理装置11221～11222に対して、対個人情報管理装置通信手段11201を介して個人情報11081の検索を要求する（ステップ1205）。

【0069】次に、認証手段11091により認証を行う（ステップ1206）。認証に失敗した場合にはその旨を利用者に通知し（ステップ1208）、対端末通信手段11061と利用者端末11031との通信を切断する（ステップ1209）。認証に成功した場合は、利用者に対応する子プロセスを起動して個人情報11081を渡す（ステップ1207）。実行制御手段11101はグループの作成が必要かどうかを判断するため、利用者の新規登録状況を確認する（ステップ1210）。グループの作成が必要な場合には、利用者グループ決定手段11141がデータベースからグループ情報を取得し（ステップ1211）、個人情報を検索してグループ情報を作成または更新する（ステップ1212）。

【0070】次に、データベース管理手段11071

が、作成または更新されたグループ情報をデータベースに保存（ステップ1213）する。グループの作成が必要ない場合には、これらの処理を行わない。次に、対端末通信手段11061により利用者端末11031との接続状況を確認する（ステップ1214）。接続している利用者端末11031がない場合は、メンテナンス実行手段11231によりメンテナンスを実行（ステップ1215）する。そして、利用者端末11031の接続要求の監視を再開する。

【0071】上記のように、本発明の第6の実施の形態においては、個人情報管理装置が、対サーバ通信手段と、対端末通信手段と、データベース管理手段と、認証手段と、固有情報管理手段と、固有情報通信手段と、利用者グループ決定手段と、一元情報検索手段と、対個人情報管理装置通信手段と、メンテナンス実行手段と、実行制御手段とを備え、利用者が接続していない場合などにデータベースの内容を確認して、個人情報やグループ情報の重複登録や矛盾などの修正といったメンテナンスを定期的または自動的に行なうようにしたので、管理者によるメンテナンス操作を軽減することが可能となる。

【0072】（第7の実施の形態）本発明の第7の実施の形態における個人情報管理装置は、対サーバ通信手段と、対端末通信手段と、データベースと、データベース管理手段と、認証手段と、固有情報管理手段と、固有情報通信手段と、利用者グループ決定手段と、固有情報特徴抽出手段と、要求予測手段と、一元情報検索手段と、対個人情報管理装置通信手段と、メンテナンス実行手段と、個人情報更新検出手段と、実行制御手段とを備え、個人情報の更新を検出し、個人情報を更新した際に関係のあるグループ情報を自動的に更新することを可能とする個人情報管理装置である。

【0073】まず、図13を参照して、本発明の第7の実施の形態における個人情報管理装置の構成を説明する。図13は本発明の第7の実施の形態における個人情報管理装置の構成を示すブロック図である。図13において、13011～13013は特定の利用者を対象にアプリケーションサービスを提供するアプリケーションサーバである。13021は個人情報13081やアプリケーション固有情報13121、およびグループ情報13151を格納するデータベースである。13031は利用者が送信するべき情報の出力とアプリケーションサーバ13011～13013が提供する情報の入力を用いる利用者端末である。13041は個人情報管理装置であり、対サーバ通信手段13051と、対端末通信手段13061と、データベース管理手段13071と、個人情報13081と、認証手段13091と、実行制御手段13101と、固有情報管理手段13111と、アプリケーション固有情報13121と、固有情報通信手段13131と、利用者グループ決定手段13141と、グループ情報13151と、固有情報特徴抽出手段

13161と、要求予測手段13171と、バッファ13181と、一元情報検索手段13191と、対個人情報管理装置通信手段13201と、アドレステーブル13211と、メンテナンス実行手段13231と、個人情報更新検出手段13241とからなる。

【0074】対サーバ通信手段13051は、ネットワークを介してアプリケーションサーバとの通信を行う手段である。対端末通信手段13061は、同様にネットワークを介して利用者端末13031との通信を行う手段である。データベース管理手段13071は、データベース13021に対して個人情報13081やアプリケーション固有情報13121、およびグループ情報13151の検索、登録、変更、削除などの操作を行う手段である。個人情報13081は、利用者のアカウント、パスワード、性別、生年月日、所属などで構成される情報である。認証手段13091は、利用者端末13031と対端末通信手段13061を介して得られた利用者のアカウントおよびパスワードと、データベースから取得した個人情報13081を用いて認証を行う手段である。

【0075】アプリケーション固有情報13121は、アプリケーションサービスにおける利用者の権限や、送受信データの履歴などで構成される情報である。固有情報管理手段13111は、アプリケーション固有情報13121と利用者の個人情報13081を対応づけて管理する手段である。固有情報通信手段13131は、アプリケーションサーバ13011～13013との間でアプリケーション固有情報13121を通信する手段である。

【0076】利用者グループ決定手段13141は、性別や年齢などの条件に該当する複数の利用者を決定する手段である。グループ情報13151は、名称、コード、管理者、条件、該当利用者などで構成される情報である。固有情報特徴抽出手段13161は、アプリケーション固有情報13121から利用者が周期的に繰り返し送受信するメッセージの特徴を抽出する手段である。要求予測手段13171は、時刻を対応づけて利用者が次に要求する情報を予測する手段である。

【0077】一元情報検索手段13191は、ネットワーク接続された他の個人情報管理装置13221～13222のネットワークアドレスを格納したアドレステーブル13211を管理して一元的な情報検索を行う手段である。対個人情報管理装置通信手段13201は、ネットワークを介して他の個人情報管理装置13221～13222との通信を行う手段である。メンテナンス実行手段13231は、データベース管理手段13071を通じてデータベース13021の内容を確認し、個人情報13081やグループ情報13151の重複登録や矛盾などをメンテナンスする手段である。

【0078】個人情報更新検出手段13241は、個人

情報13081を監視して内容が更新されたことを検出する手段である。実行制御手段13101は、個人情報13081の更新を検出し、関係のあるグループ情報13151を自動的に更新するよう、対サーバ通信手段13051、対端末通信手段13061、データベース管理手段13071、認証手段13091、固有情報管理手段13111、固有情報通信手段13131、利用者グループ決定手段13141、固有情報特徴抽出手段13161、要求予測手段13171、一元情報検索手段13191、対個人情報管理装置通信手段13201、メンテナンス実行手段13231、個人情報更新検出手段13241の実行を制御する手段である。

【0079】次に、図14を参照して、本発明の第7の実施の形態における個人情報管理装置の動作を説明する。図14は図13に示す本発明の第7の実施の形態における個人情報管理装置の処理の流れを示すフローチャートである。なお、図14の処理フローは、図12に示す、第6の実施の形態の処理フローとの相違点を説明するためのもので、図12のステップ1207で起動される子プロセスの処理フローである。なお、図14中の1451、1452、…、1464は処理手順の番号である。まず、図14の処理フローの理解を容易にするために、図12を参照してステップ1201からステップ1207までの処理フローを説明する。従って、図14の説明は、以下図12の説明から開始する。なお、図12の説明においては、図13の各構成部を使用するため、図13の構成部の符号を使用する。

【0080】まず、個人情報管理装置13041が起動すると、実行制御手段13101が処理を開始し（ステップ1201）、対端末通信手段13061が利用者端末13031からの接続要求受信を監視する（ステップ1202）。接続要求を受信すると、データベース管理手段13071を用いてデータベース13021から該当する利用者の個人情報を検索し（ステップ1203）、結果を確認する（ステップ1204）。該当する個人情報が存在しない場合には、一元情報検索手段13191により、アドレステーブル13211に登録されている他の個人情報管理装置13221～13222に対し、対個人情報管理装置通信手段13201を介して個人情報の検索を要求する（ステップ1205）。

【0081】次に、認証手段13091により認証を行う（ステップ1206）。認証に失敗した場合にはその旨を利用者に通知し（ステップ1208）、対端末通信手段13061と利用者端末13031との通信を切断する（ステップ1209）。認証に成功した場合は、利用者に対応する子プロセスを起動して子プロセスに対し個人情報13081を渡す（ステップ1207）。

【0082】そこで、図14の処理フローへ進み、起動された子プロセスは処理を開始し（ステップ1451）て、対端末通信手段13061と対サーバ通信手段13

051におけるデータ受信を監視する（ステップ1452）。データを受信した場合は、送信先を確認し（ステップ1453）、アプリケーションサーバ13011～13013に対する送信データ（情報要求）であれば、バッファ13181に該当情報があるかどうかを確認し（ステップ1454）、あればそれを対端末通信手段13061によって送信する（ステップ1456）。該当情報がない場合は、認証情報を付加して対サーバ通信手段13051により送信し（ステップ1455）、アプリケーション固有情報13121の必要性を確認し（ステップ1457）、必要な場合には固有情報通信手段13131が対サーバ通信手段13051を使用して送受信を行う（ステップ1458）。

【0083】また、利用者端末13031への送信データであれば対端末通信手段13061により送信する（ステップ1456）。次に、要求予測手段13171が時刻及び固有情報に基いて予測した要求によりアプリケーションサーバ13011～13013からデータを受信し、バッファ13181に格納する（ステップ1459）。利用者端末13031との接続状況を確認し（ステップ1460）、接続されている場合にはデータ通信処理（ステップ1452～1460）を繰り返し実行する。利用者端末13031との接続が切断された場合には、個人情報更新検出手段13241により個人情報13081の更新を確認する（ステップ1461）。個人情報13081が更新されている場合には、メンテナンス実行手段13231により関係のあるグループ情報13151に対するメンテナンスを実行する（ステップ1462）。そして、データベース管理手段13071により、個人情報13081をデータベース13021に保存し（ステップ1463）処理を終了する（ステップ1464）。

【0084】上記のように、本発明の第7の実施の形態においては、個人情報管理装置が、対サーバ通信手段と、対端末通信手段と、データベース管理手段と、認証手段と、固有情報管理手段と、固有情報通信手段と、利用者グループ決定手段と、一元情報検索手段と、対個人情報管理装置通信手段と、メンテナンス実行手段と、個人情報更新検出手段と、実行制御手段とを備え、個人情報を更新した際に関係のあるグループ情報を自動的に更新することができるよう構成したことにより、メンテナンス操作を軽減することができる。

#### 【0085】

【発明の効果】本発明は、上記のように構成され、特に利用者の認証により個人情報に基づき得られた認証情報をアプリケーションサーバに対する送信データに付加するようにしたことにより、複数のアプリケーションサービスを利用する場合に、一度認証を行うのみでアプリケーションサーバ毎に認証処理を必要とせず、複数のアプリケーションサービスを使用する場合における利用者の

操作負担を軽減することができる。

【0086】また、本発明は、特に個々のアプリケーションサービスに固有のアプリケーション固有情報を利用者の個人情報と対応づけて管理するようにしたことにより、利用者と個々のアプリケーションサーバとの間の固有の操作を軽減することができる。

【0087】また、本発明は、特に新たな利用者の登録があった場合に、グループ情報を自動的に作成または更新するようにしたことにより、グループを対象に情報提供を行う場合、情報を配信したい複数の利用者を選別する処理を軽減することができる。

【0088】また、本発明は、特にアプリケーション固有情報から利用者が周期的に繰り返し送受信するメッセージの特徴を抽出し、その時刻を対応づけて利用者が次に要求する情報を予測するようにしたことにより、要求される情報を利用者の操作に先行して受信し利用者の応答待ち時間を短縮することができる。

【0089】また、本発明は、特に利用者からの接続要求を受信した際に、必要に応じ、自動的に他の個人情報管理装置に対して個人情報の検索を要求するようにしたことにより、利用者は自己の個人情報の格納先を意識することなく、任意の個人情報管理装置に接続することができるので、移動した利用者が異なる利用者端末から接続したような場合でも、同一のアプリケーションサービスを受けることができる。

【0090】また、本発明は、特に利用者が接続していない場合などにデータベースの内容を自動的に確認して、個人情報やグループ情報の重複登録や矛盾等の修正のようなメンテナンスを定期的または自動的に行うようにしたことにより、管理者によるメンテナンス操作の軽減を図ることができる。

【0091】また、本発明は、特に個人情報を更新した際に、関係のあるグループ情報を自動的に更新することができるようしたことにより、メンテナンス操作を軽減することができる。

#### 【図面の簡単な説明】

【図1】本発明の第1の実施の形態における個人情報管理装置の構成を示すブロック図、

【図2】図1に示す本発明の第1の実施の形態における個人情報管理装置の処理の流れを示すフローチャート、

【図3】本発明の第2の実施の形態における個人情報管理装置の構成を示すブロック図、

【図4】図3に示す本発明の第2の実施の形態における個人情報管理装置の処理の流れを示すフローチャート、

【図5】本発明の第3の実施の形態における個人情報管理装置の構成を示すブロック図、

【図6】図5に示す本発明の第3の実施の形態における個人情報管理装置の処理の流れを示すフローチャート、

【図7】本発明の第4の実施の形態における個人情報管理装置の構成を示すブロック図、

【図8】図7に示す本発明の第4の実施の形態における個人情報管理装置の処理の流れを示すフローチャート、

【図9】本発明の第5の実施の形態における個人情報管理装置の構成を示すブロック図、

【図10】図9に示す本発明の第5の実施の形態における個人情報管理装置の処理の流れを示すフローチャート、

【図11】本発明の第6の実施の形態における個人情報管理装置の構成を示すブロック図、

【図12】図11に示す本発明の第6の実施の形態における個人情報管理装置の処理の流れを示すフローチャート、

【図13】本発明の第7の実施の形態における個人情報管理装置の構成を示すブロック図、

【図14】図13に示す本発明の第7の実施の形態における個人情報管理装置の処理の流れを示すフローチャート。

【符号の説明】

1011、1012 アプリケーションサーバ

1021 データベース

1031 利用者端末

1041 個人情報管理装置

1051 対サーバ通信手段

1061 対端末通信手段

1071 データベース管理手段

1081 個人情報

1091 認証手段

1101 実行制御手段

3011～3013 アプリケーションサーバ

3021 データベース

3031 利用者端末

3041 個人情報管理装置

3051 対サーバ通信手段

3061 対端末通信手段

3071 データベース管理手段

3081 個人情報

3091 認証手段

3101 実行制御手段

3111 固有情報管理手段

3121 アプリケーション固有情報

3131 固有情報通信手段

5011～5013 アプリケーションサーバ

5021 データベース

5031 利用者端末

5041 個人情報管理装置

5051 対サーバ通信手段

5061 対端末通信手段

5071 データベース管理手段

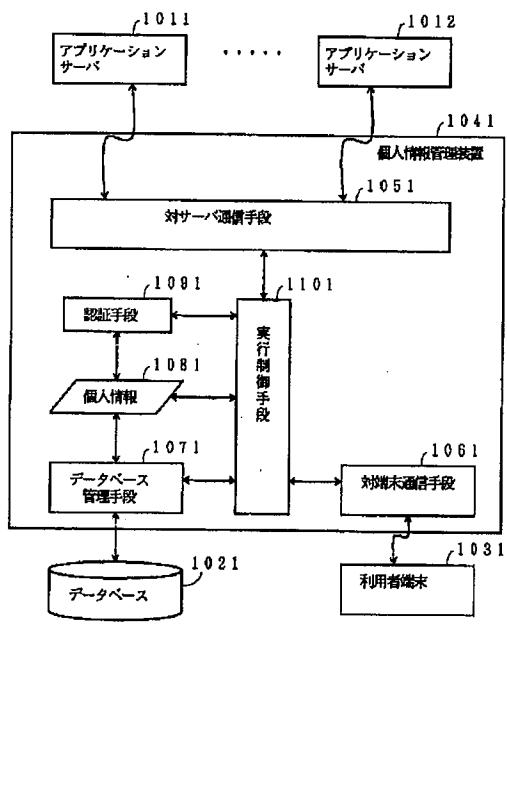
5081 個人情報

5091 認証手段

5101 実行制御手段  
5111 固有情報管理手段  
5121 アプリケーション固有情報  
5131 固有情報通信手段  
5141 利用者グループ決定手段  
5151 グループ情報  
7011～7013 アプリケーションサーバ  
7021 データベース  
7031 利用者端末  
7041 個人情報管理装置  
7051 対サーバ通信手段  
7061 対端末通信手段  
7071 データベース管理手段  
7081 個人情報  
7091 認証手段  
7101 実行制御手段  
7111 固有情報管理手段  
7121 アプリケーション固有情報  
7131 固有情報通信手段  
7141 利用者グループ決定手段  
7151 グループ情報  
7161 固有情報特徴抽出手段  
7171 要求予測手段  
7181 バッファ  
9011～9013 アプリケーションサーバ  
9021 データベース  
9031 利用者端末  
9041 個人情報管理装置  
9051 対サーバ通信手段  
9061 対端末通信手段  
9071 データベース管理手段  
9081 個人情報  
9091 認証手段  
9101 実行制御手段  
9111 固有情報管理手段  
9121 アプリケーション固有情報  
9131 固有情報通信手段  
9141 利用者グループ決定手段  
9151 グループ情報  
9161 固有情報特徴抽出手段  
9171 要求予測手段  
9181 バッファ  
9191 一元情報検索手段  
9201 対個人情報管理装置通信手段  
9211 アドレステーブル  
9221～9222 (他) 個人情報管理装置  
11011～11013 アプリケーションサーバ  
11021 データベース  
11031 利用者端末  
11041 個人情報管理装置

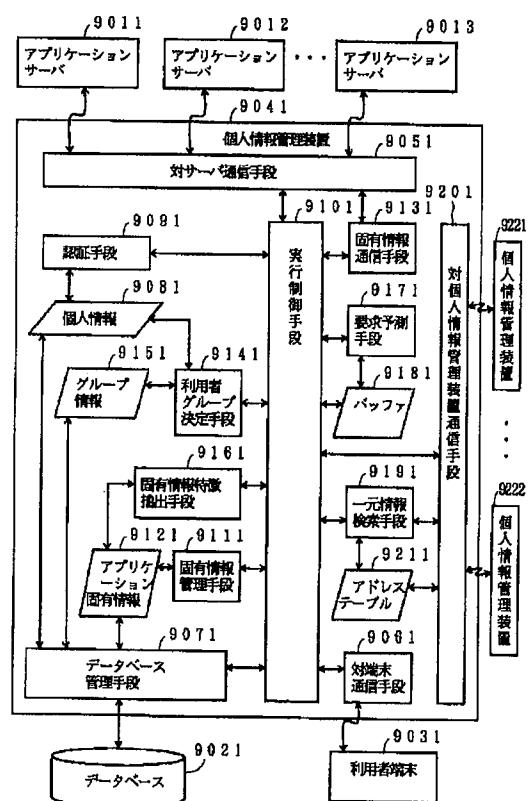
11051 対サーバ通信手段  
 11061 対端末通信手段  
 11071 データベース管理手段  
 11081 個人情報  
 11091 認証手段  
 11101 実行制御手段  
 11111 固有情報管理手段  
 11121 アプリケーション固有情報  
 11131 固有情報通信手段  
 11141 利用者グループ決定手段  
 11151 グループ情報  
 11161 固有情報特徴抽出手段  
 11171 要求予測手段  
 11181 バッファ  
 11191 一元情報検索手段  
 11201 対個人情報管理装置通信手段  
 11211 アドレステーブル  
 11221～11222 (他) 個人情報管理装置  
 11231 メンテナンス実行手段  
 13011～13013 アプリケーションサーバ  
 13021 データベース  
 13031 利用者端末

【図1】

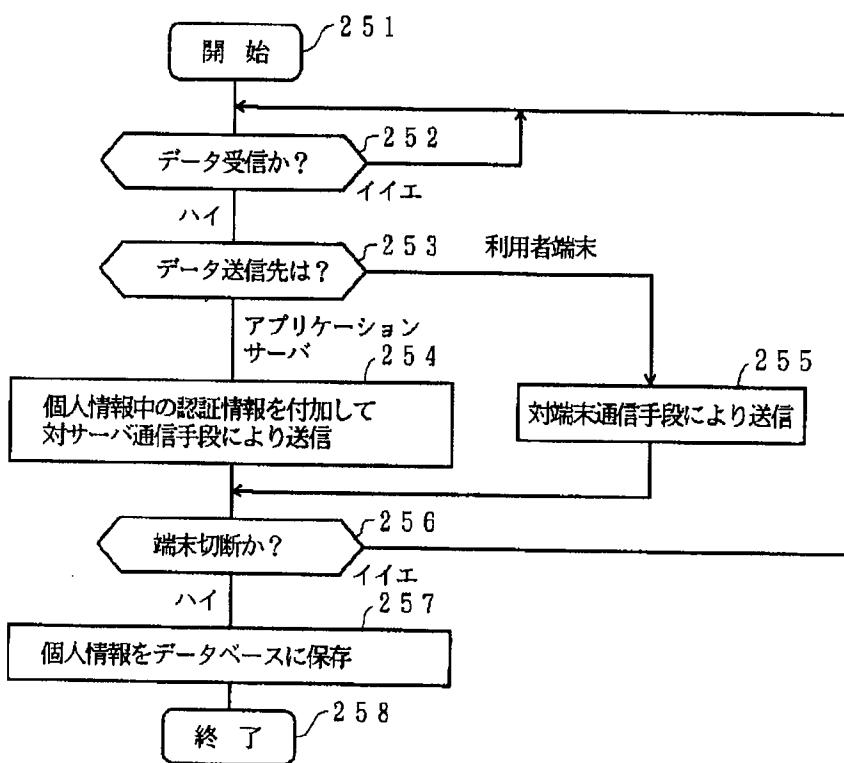
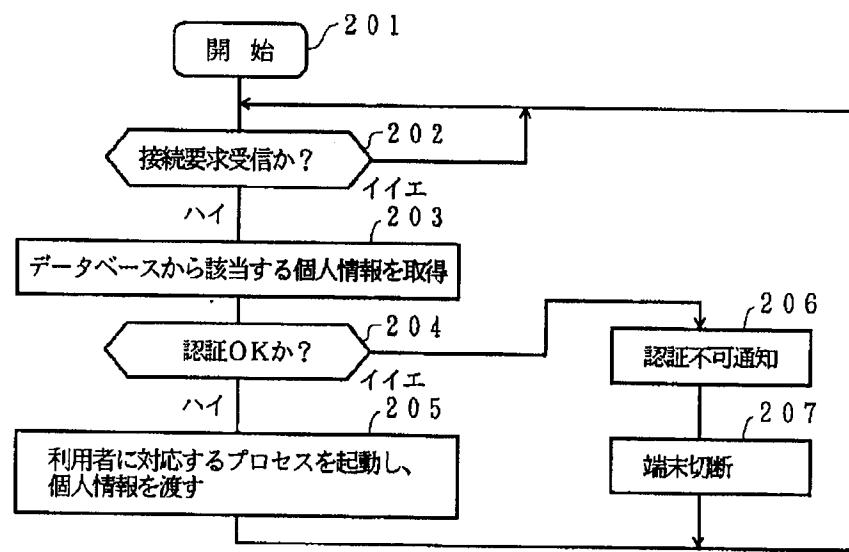


13041 個人情報管理装置  
 13051 対サーバ通信手段  
 13061 対端末通信手段  
 13071 データベース管理手段  
 13081 個人情報  
 13091 認証手段  
 13101 実行制御手段  
 13111 固有情報管理手段  
 13121 アプリケーション固有情報  
 13131 固有情報通信手段  
 13141 利用者グループ決定手段  
 13151 グループ情報  
 13161 固有情報特徴抽出手段  
 13171 要求予測手段  
 13181 バッファ  
 13191 一元情報検索手段  
 13201 対個人情報管理装置通信手段  
 13211 アドレステーブル  
 13221～13222 (他) 個人情報管理装置  
 13231 メンテナンス実行手段  
 13241 個人情報更新検出手段

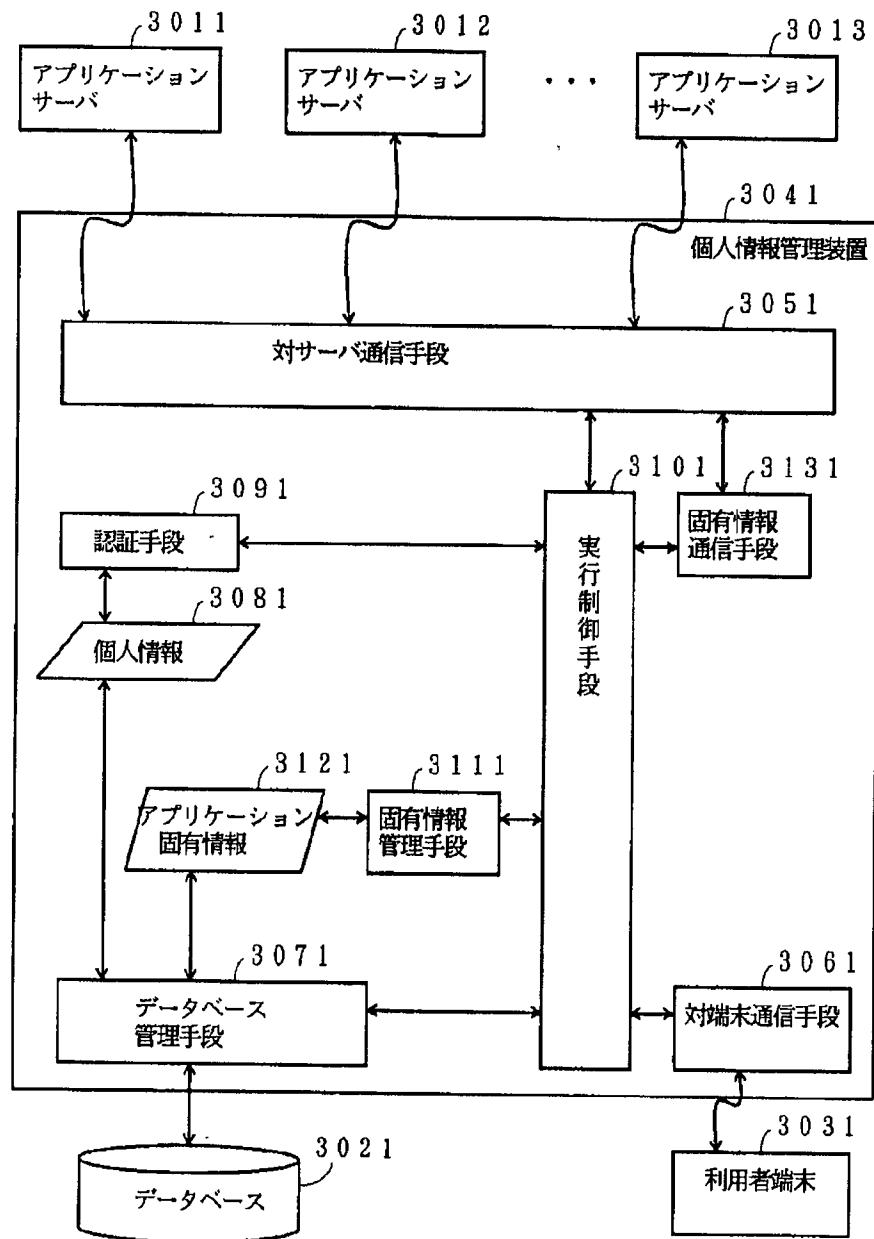
【図9】



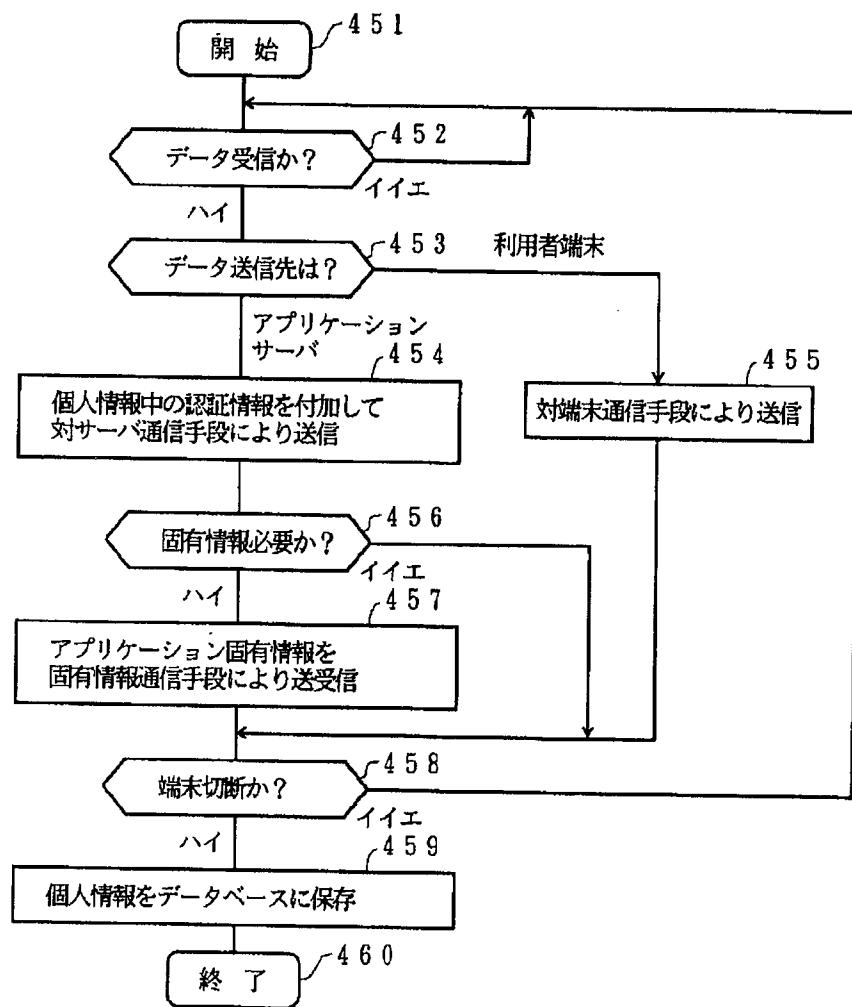
【図2】



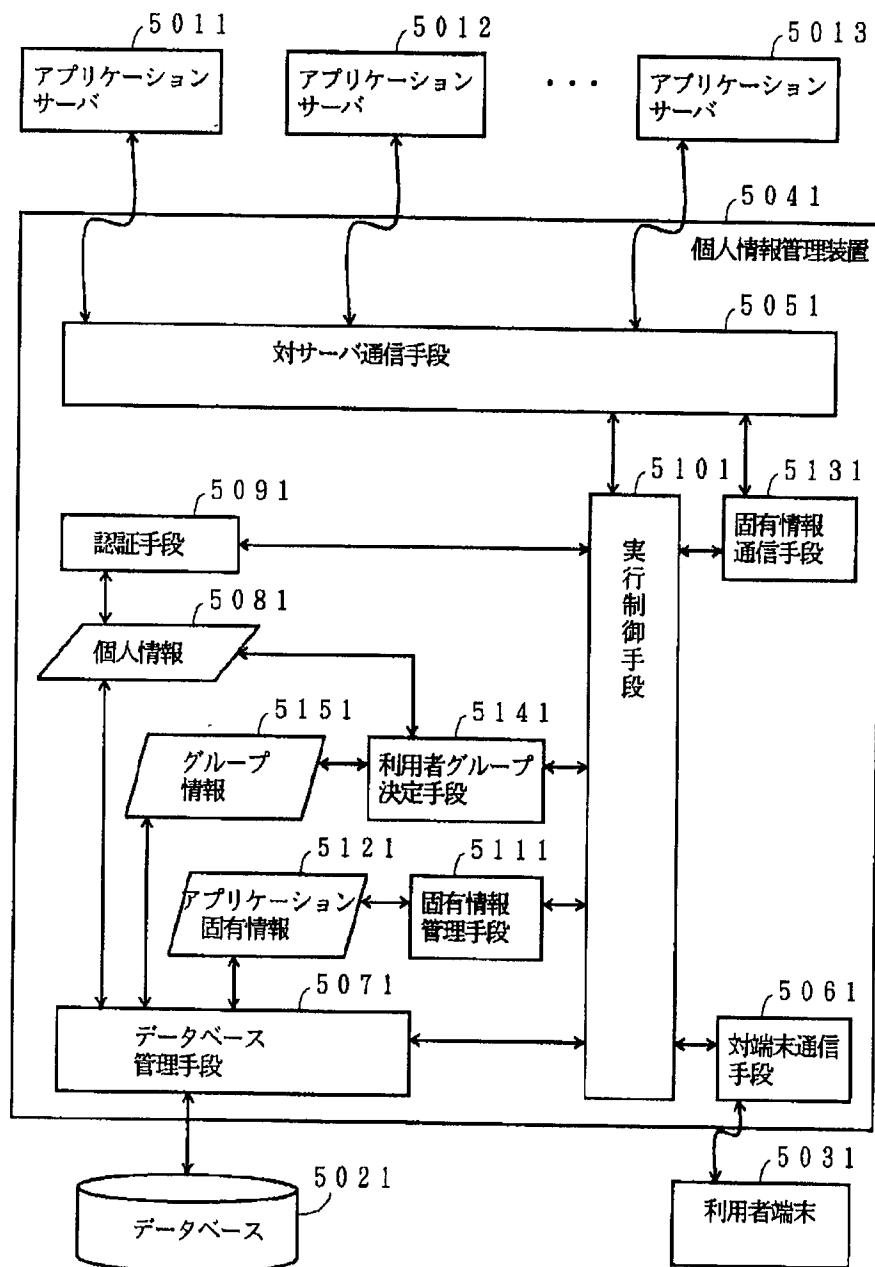
【図3】



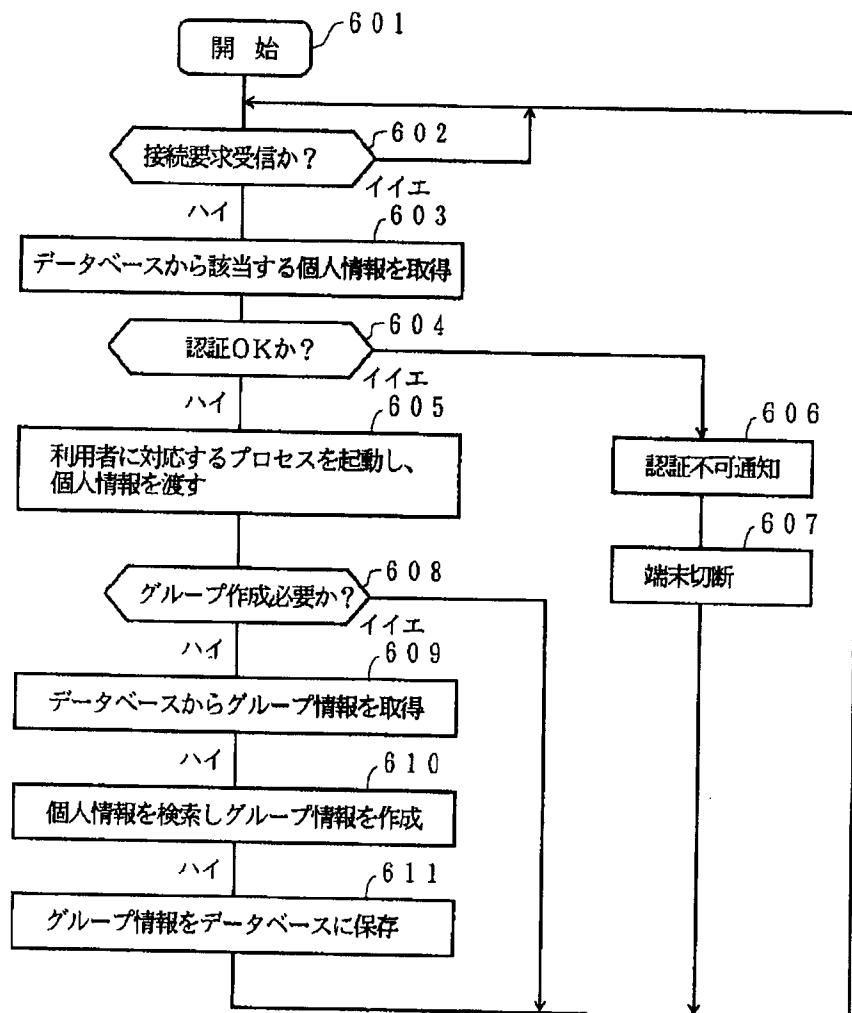
【図4】



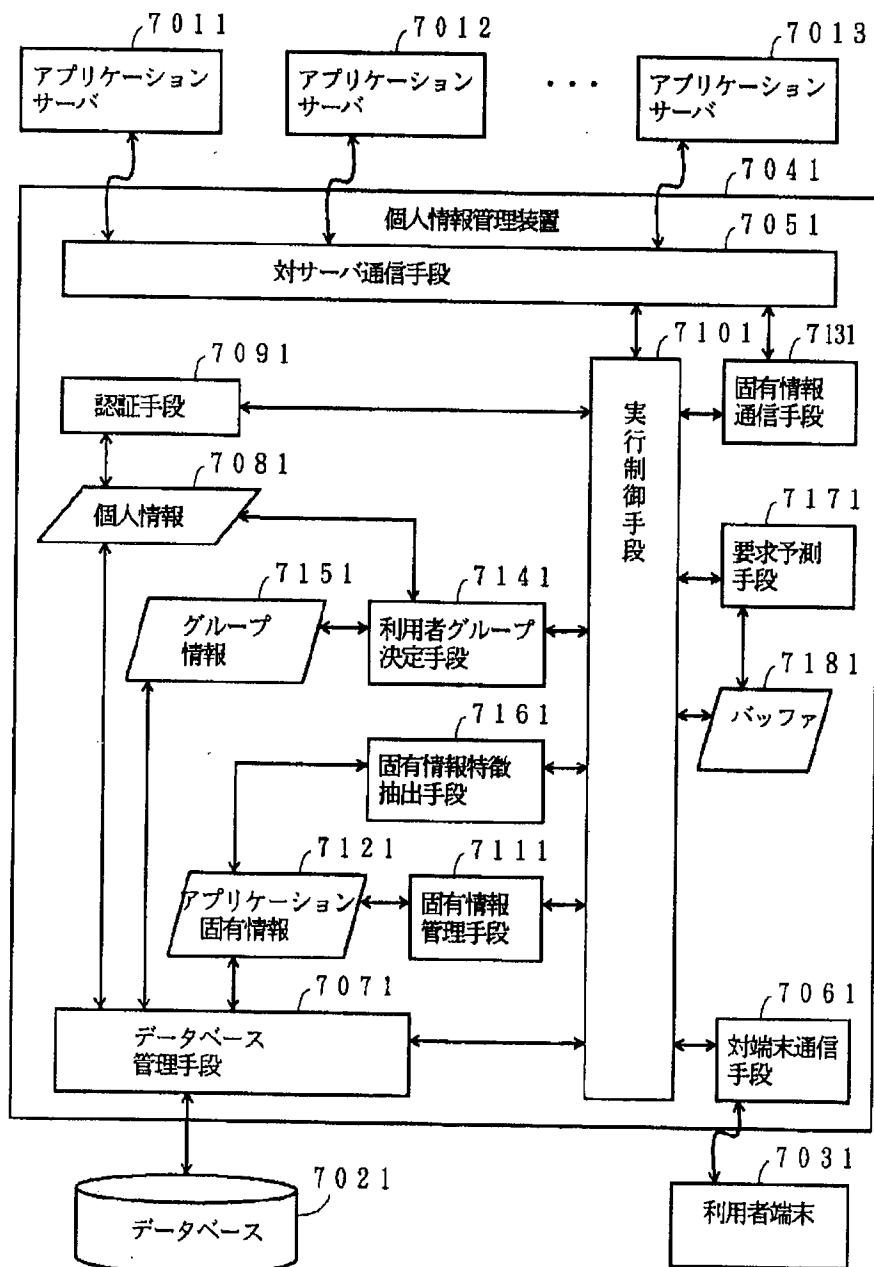
【図5】



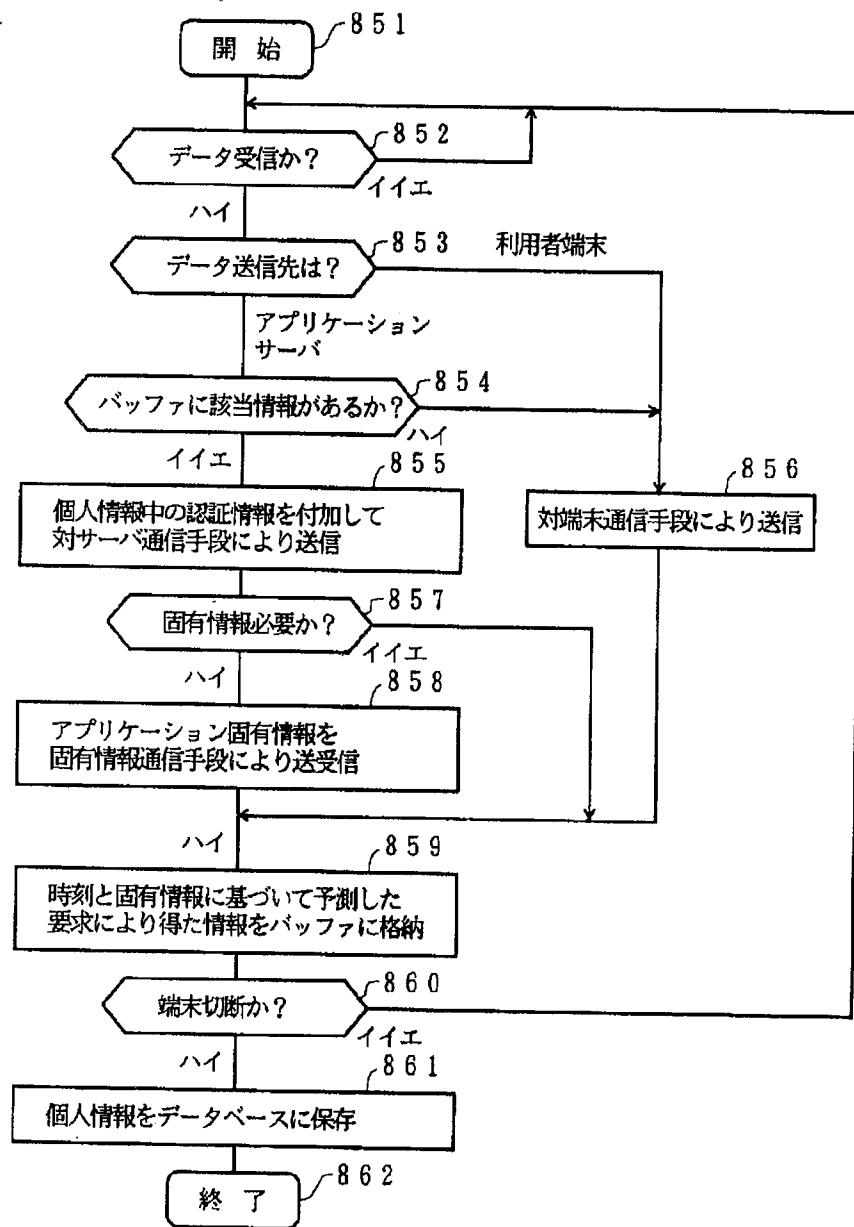
【図6】



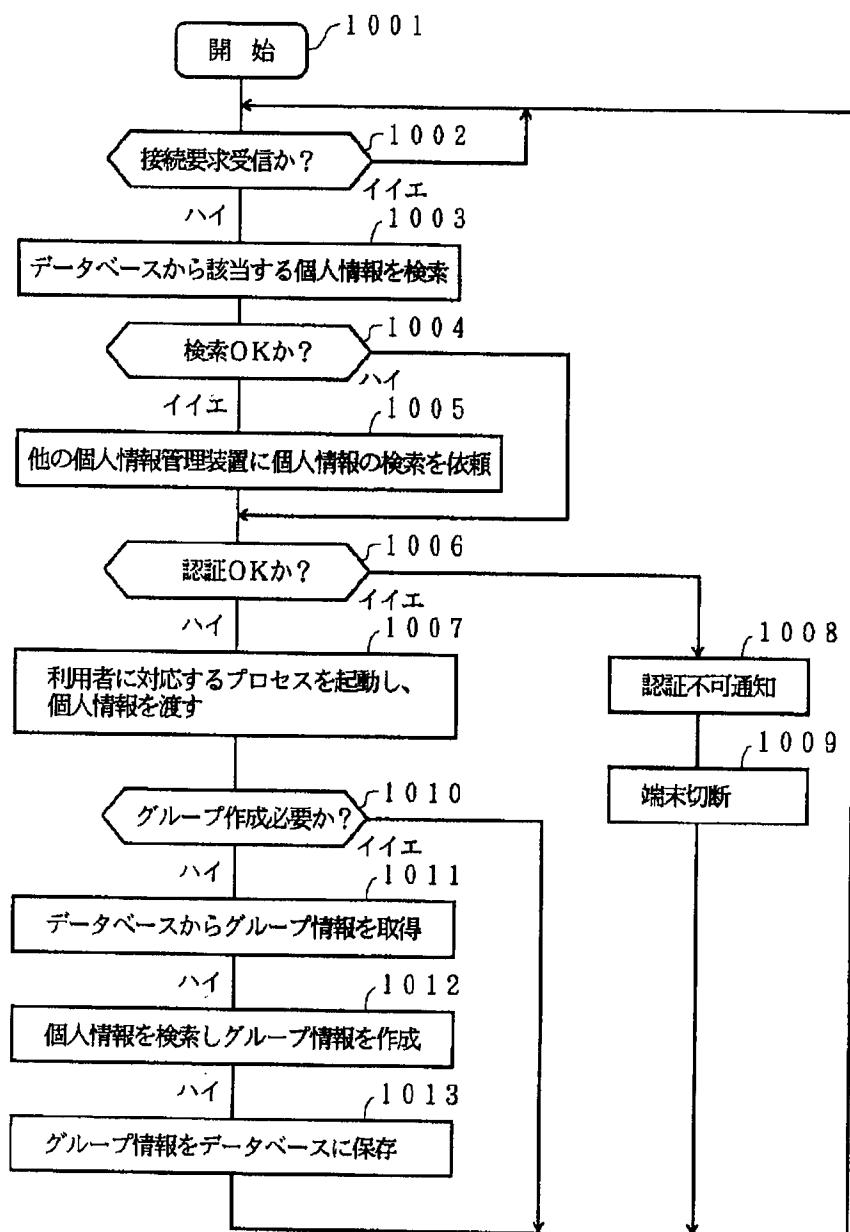
【図7】



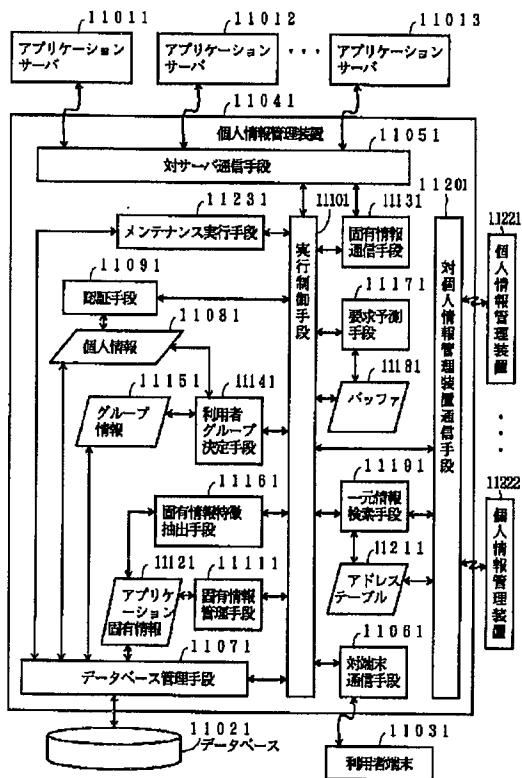
【図8】



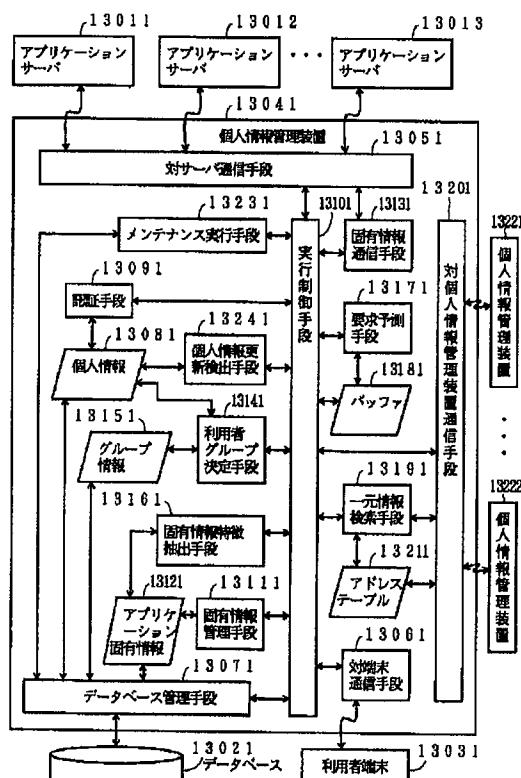
【図10】



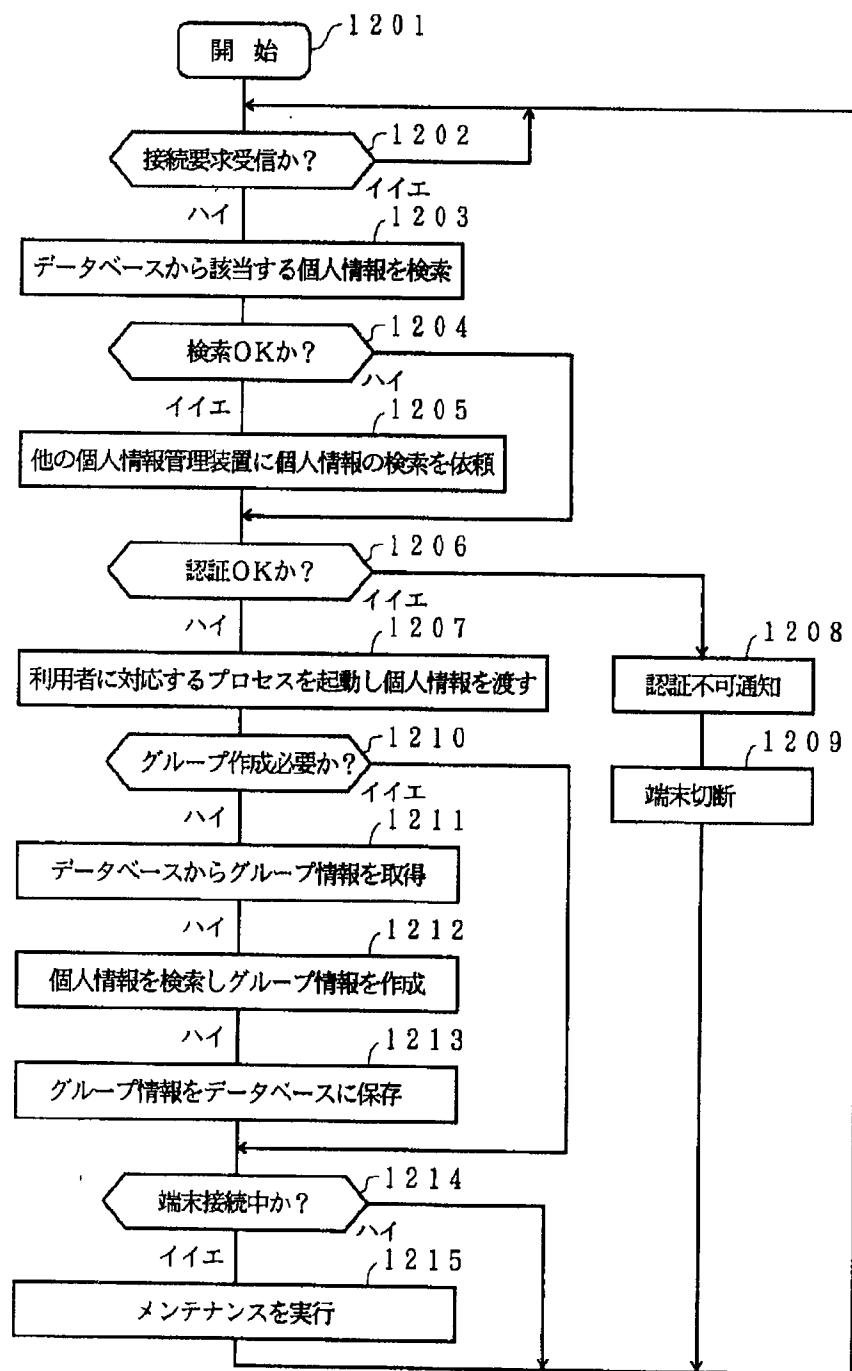
【図1.1】



【図1.3】



【図12】



【図14】

